

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, David Albers, being duly sworn, depose and state as follows:

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the: (1) the premises known as 206 North Morse Avenue, Apartment 36, Liberty, Missouri, hereinafter "**PREMISES**," as further described in **Attachment A-1**; and (2) the person of Zachary **BALLARD**, as further described in **Attachment A-2**, for the things described in **Attachment B**.

2. I am currently employed as a detective with the Kansas City, Missouri Police Department and serving as a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI). I have been employed with the Kansas City, Missouri Police Department since March 1998, and am currently assigned to the FBI Child Exploitation Task Force, Kansas City, Missouri. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. Since May 2013, I have been assigned to investigate computer crimes to include violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training such as the annual Crimes Against Children Conference and Innocent Images training provided by the FBI. These trainings have included instruction related to the laws against sexual abuse of minors, online applications used to entice children to produce sexually explicit material or engage in sexually explicit conduct with adults, and other subjects related to offenses committed against minor children.

3. I have assisted in the investigation of hundreds of child pornography cases. At all times throughout this affidavit, I use the term "child pornography" merely as shorthand to refer to

visual depictions of actual minors engaged in sexually explicit conduct. During that time, I have had to view thousands of images of child pornography. I use the terms “visual depiction,” “minor,” and “sexually explicit conduct” as those terms are defined in 18 U.S.C. § 2256. I have previously applied the federal definition of child pornography used in this affidavit to dozens of search warrant applications and in dozens of grand jury presentations.

4. Since this affidavit is being submitted for the limited purpose of showing that there is probable cause for the requested warrant, I have not included each and every fact known to me concerning this investigation.

#### **STATUTORY AUTHORITY**

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. §§ 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production

of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. §§ 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

e. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has

been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. As discussed herein, there is probable cause to search the **PREMISES**, and **BALLARD** for evidence of the Subject Offenses, as further described in Attachment B.

**STATEMENT OF FACTS SUPPORTING PROBABLE CAUSE**

7. On Tuesday, March 9, 2021, an FBI online covert employee (OCE) was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. OCE directed the investigative focus to a device at IP address 70.94.34.179, because it was associated with a torrent which was identified as having files of investigative interest to child pornography investigations.

8. Using a computer running investigative BitTorrent software, OCE directly connected to the device at IP address 70.94.34.179, hereinafter referred to as "Suspect Device". The "Suspect Device" reported it was using BitTorrent client software -FW6842- FrostWire/6.8.4 libtorrent/1.2.3.0.

9. The torrent had the infohash: 89c61853e871ea7684ce9b4f96fe048acb6c6b07 and referenced 689 files. Between 5:51 a.m. and 10:36 a.m., OCE successfully completed the download of approximately 224 image files from the torrent that the "Suspect Device" was making available. The sexually explicit files depicted apparent prepubescent females. Some of the images included a lascivious exhibition of nude prepubescent female's genitals. Many other images depicted an adult male hand exposing the prepubescent female's genitals while they appeared to be sleeping by altering clothing and using his fingers to manipulate the vagina.

Several other images depicted an adult male sexually abusing minor females by having intercourse and having the females perform oral sex. For example, image “000496” depicts an adult male vaginally penetrating a prepubescent female with his penis and image “000610” depicts a prepubescent female performing oral sex on an apparent adult male.

10. The Suspect Device at IP Address 70.94.34.179 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

11. On March 10, 2021, your affiant conducted a query through the American Registry for Internet Numbers (ARIN). ARIN reported the IP address 70.94.34.179 to be registered to Charter Communications, Inc. An administrative subpoena was served for Charter to disclose the subscriber information for the IP address. On March 16, 2021, Charter’s response indicated the subscriber information was as follows: Zachary **BALLARD** of 206 North Morse Avenue, Apartment 36, Liberty, Missouri 64068, and email ‘branchoptics@hotmail.com’.

12. On Wednesday, March 17, 2021, and Thursday, March 18, 2021, your affiant initiated a physical surveillance in the vicinity of the **PREMISES**. The apartment appeared to be a one-bedroom unit. The mailbox for the **PREMISES** displayed the name “Z **Ballard**”. According to open source database checks, **BALLARD** showed to reside at the apartment for several years. There are no other names associated with the **PREMISES**. All available Wi-Fi Internet networks were password protected.

13. On March 23, 2021, your affiant conducted physical surveillance and observed a white, Mitsubishi Galant, bearing Missouri license plate RD8 M7V registered to Zachary **BALLARD** was observed parked at the multi-family apartment building parking lot. The male held and used a cell phone before exiting the vehicle. The physical description of the male was consistent with **BALLARD**’s Missouri driver’s license. The male entered the **PREMISES**. No

other persons were observed coming or going from the apartment during any of the physical surveillance conducted.

14. FrostWire is a client of Bit Torrent. Your affiant's data logs indicate the suspect device used version FrostWire/6.8.4 libtorrent/a.2.3.0 at the time of distribution of the sexually explicit files noted above. According to the FrostWire website and GitHub (Git is software for tracking changes in any set of files, usually used for coordinating work among programmers collaboratively developing source code during software development), the FrostWire 6.8.4 versions is associated with Windows and Mac devices and the libtorrent 1.2.3.0 is associated with Android devices.

15. There is probable cause to believe that the computer(s) (as defined in this affidavit), or other electronic device(s) (*i.e.*, tablet, smartphone and other devices subsumed within the definition of "computer") used to access the BitTorrent network may well have been a mobile electronic device capable of accessing the internet. Such mobile devices like smartphones and tablets have become increasingly popular and have supplanted, to a significant degree, traditional laptop or desktop computer as the hardware used by people to access the internet. This popularity is driven by the ease of use of such mobile devices, *i.e.*, the short amount of time required to boot up the mobile devices and the mobile devices' easy portability. I know from my training and experience that people often keep mobile electronic devices such as smartphones on their person, such as in their pockets or in handbags. This closeness of the mobile device (such as a smartphone) to the person is important to the mobile device's utility, as it is this closeness that allows the user to hear message alerts, to respond to telephone calls, to compose and send messages such as texts and emails, and to quickly access the internet. Users of such mobile devices often go through their days receiving and sending a large number of text messages (including by means

of a variety of messages applications) and email messages on a continuous basis, making it critical that the mobile device remain on the person of the user throughout the day. As a result, a mobile device that could have accessed the BitTorrent network, using the **PREMISES'** wireless connection (as opposed to a cellular data connection), may well be on the person of Zachary **BALLARD**.

### **DEFINITIONS**

16. The following definitions apply to this Affidavit and to Attachment B to this Affidavit:

a. "Child Erotica," as used herein, means materials demonstrating a sexual interest in minors, including fantasy narratives, cartoons, and books describing or alluding to sexual activity with minors, sexual aids, children's clothing catalogues, and child modeling images.

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

d. "Internet Protocol address" (or simply "IP address") is a unique numeric address used by computers on the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

e. "The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. “Computer software,” as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

k. Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.



**BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY**

17. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, including cellphones, and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers, including cellphones, basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash”

drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. Based upon my training and experience and information relayed to me by

agents and others involved in the forensic examination of computers, I know that mobile device users often connect to known wireless networks which are available to them, especially localized networks within their residence. The connection information such as usernames and passwords are typically stored within the device and the device automatically connects when within range of a known wireless network. Individuals often set this automatic connect preference in their devices in order to conserve battery consumption, improve connection speeds, and reduce cellular data consumption which is often limited or metered. Mobile devices connected to a wireless network will often share the same IP address information as reported by the residential wireless network provider.

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

18. The storage capacity of the electronic storage media used in home computers and cell phones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

19. A user can set up an online storage account from any computer or cell phone with access to the Internet. Evidence of such online storage of child pornography is often found on the

user's computer or cell phone. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or cell phone in most cases.

20. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users.

21. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file.

22. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer

and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

23. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file came from one or more IP addresses. Such Software monitors and logs Internet and local network traffic.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

24. Searches and seizures of evidence from cellular phones commonly require agents to download or copy information from the cellular phone to be processed later in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or

destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

25. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any application software that may have been used to create the data (whether stored on hard drives or on external media).

#### **SEARCH METHODOLOGY TO BE EMPLOYED**

26. The search procedure of electronic data contained in computer hardware, computer software, memory storage devices, and/or cell phones may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, memory storage devices, and/or cell phone to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE  
DISTRIBUTION, RECEIPT, OR POSSESSION OF CHILD PORNOGRAPHY  
OR IN THE CONSPIRACIES OR ATTEMPTS TO COMMIT THOSE CRIMES**

27. As set forth above, probable cause exists to believe that an individual residing at the **PREMISES** has distributed, received, or possessed child pornography, or has conspired or attempted to commit these crimes. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute or possess child pornography, or who conspire or attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes often possess and maintain their "hard copies" of child

pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondences, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. **These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.**

d. Likewise, those who distribute or possess child pornography, or who attempt or conspire to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. **These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.**

e. Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individual with whom they have been in contact and who share the same interests in child pornography.


f. **Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.**



**CONCLUSION**

28. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that the individual more fully described in **Attachment A-2**, who resides at the **PREMISES** more fully described in **Attachment A-1**, is involved in the distribution, receipt, and/or possession of child pornography, in violation of 18 U.S.C. § 2252. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. § 2252 (distribution, receipt, and possession of child pornography), is located on the person of **BALLARD**, and the **PREMISES** described above, and this evidence, listed in **Attachment B** to this affidavit, which is incorporated herein by reference, is contraband or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

29. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the **PREMISES** described in **Attachment A-1** and the person described in **Attachment A-2**, and seizure and search of the items listed in **Attachment B**.

  
\_\_\_\_\_  
David Albers  
Task Force Officer  
Federal Bureau of Investigation

Sworn and subscribed to before me via reliable electronic means this 29th day of March 2021.

By telephone at 4:16 pm

  
\_\_\_\_\_  
HONORABLE W. BRIAN GADDY  
United States Magistrate Judge  
Western District of Missouri.

